Mobile Application Fraud

กรณีศึกษาคดีเหยื่อมิจฉาชีพถูกหลอกลวงให้ติดตั้งแอปพลิเคชันไม่พึงประสงค์
ในอุปกรณ์สื่อสารเคลื่อนที่ จนทำให้เสียทรัพย์

กลุ่มตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ กองตรวจพิสูจน์ทางวิทยาศาสตร์ สถาบันนิติวิทยาศาสตร์

What is Digital Forensics?

Cybercrime

- also called computer crime
- the use of a computer as an instrument to further illegal ends
- such as committing fraud, stealing identities, trafficking in child pornography and intellectual property, or violating privacy.

Assets

Top 5 cyber crimes?

5 top cybercrimes in 2023:

Phishing Scams.
Website Spoofing.
Ransomware.
Malware.
IOT Hacking.

Assets

Business process to tracking

Issuing Counterfeit Cheque

A fake cheque having inordinate amounts can be issued to gullible participants in a number of frauds such as lottery scams, cheque over-payment schemes, internet auctions, and other similar scams.

Criminals can also steal a cheque, endorse it and present it for payment at a retail location or at the bank teller window using bogus personal identification.

Internet Banking and Related Frauds

Triangulation/Site cloning

- Customers enter their card details on fraudulent shopping sites. These details are then misused.

Hacking

- Unauthorized access to the card management platform of banking system.
- Counterfeit cards are then issued for the purpose of money laundering.

Lost / Stolen Card

- It refers to the use of a card lost by a legitimate account holder for unauthorized purposes.

Identity Theft

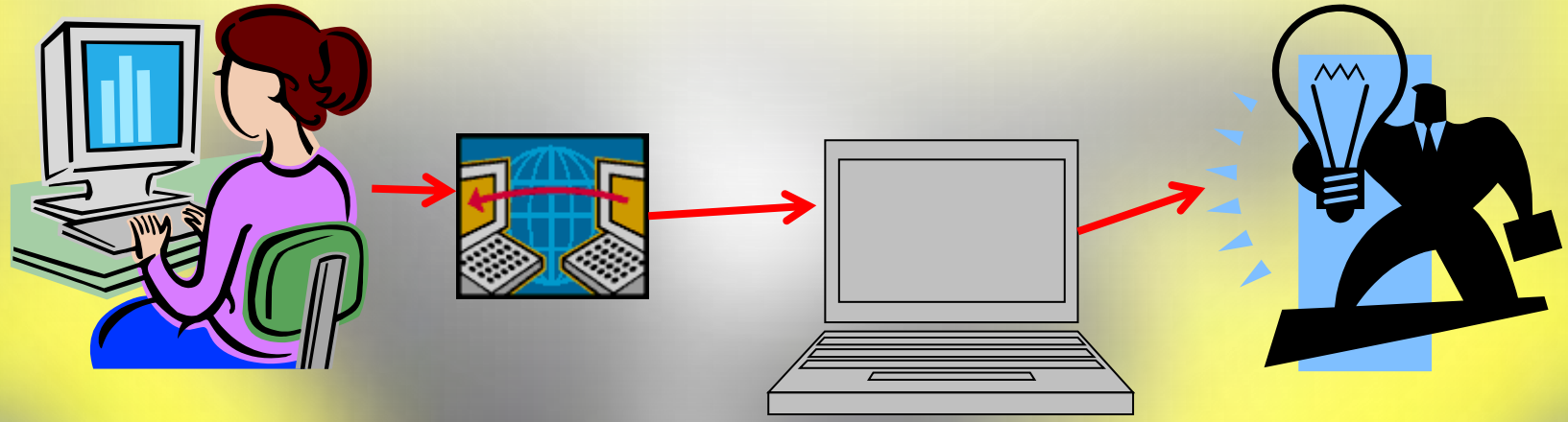
Fraudsters can steal your identity by deploying hostile software programs or conducting malware attacks, phishing, SMS-ishing and whaling apart from stealing confidential data.

For example, you might receive an unauthorized email in your inbox, asking for your account details, under the pretext of updating bank records.

What is Digital Forensics?

คำถามที่ต้องตอบ

เงื่อนไขของกฎหมาย



Who What Where When How Why

“ภัยคุกคามในการใช้แอปพลิเคชันมือถือหมายถึงการเผชิญกับความเสี่ยงหลายประการที่ผู้ใช้แอปพลิเคชันมือถือต้องระมัดระวัง
ภัยคุกคามนี้สามารถมีลักษณะทุจริตหรือเป็นเหตุการณ์ที่ทำให้เสี่ยงต่อข้อมูลส่วนตัว, ความเป็นส่วนตัว, หรือทรัพย์สินทางปัญญาของผู้ใช้”

ตัวอย่าง

การโจมตีฟิชชิ่ง (Phishing Attacks): ผู้ไม่หวังดีส่งข้อความหรืออีเมลปลอมเพื่อหลอกลวงผู้ใช้ให้ใส่ข้อมูลส่วนตัว เช่นรหัสผ่านหรือข้อมูลบัตรเครดิต.

การสร้างแอปปลอม (Fake Apps): การสร้างแอปพลิเคชันปลอมที่ดูเหมือนแอปที่ถูกต้องเพื่อหลอกผู้ใช้ที่จะดาวน์โหลด และใส่ข้อมูลส่วนตัว.

มัลแวร์และสไปแวร์ (Malware and Spyware): การติดตั้งซอฟต์แวร์ที่ไม่พึงประสงค์ที่สามารถทำลายข้อมูลหรือดูข้อมูลส่วนตัวได้.

การถูกโจมตีจากระยะไกล (Remote Attacks): การโจมตีที่เป้าหมายเป็นแอปพลิเคชันหรือระบบปฏิบัติการมือถือจากระยะไกลเพื่อให้ผู้ไม่หวังดีได้รับควบคุม

การขโมยข้อมูลผู้ใช้ (Account Takeover): การดักรับหรือขโมยข้อมูลเข้าสู่ระบบผู้ใช้ เพื่อนำไปใช้โดยไม่ได้รับอนุญาต.

การปลอมแปลงแอปพลิเคชันอย่างอื่น: การปลอมแปลงหรือการทำทรัพย์สินทางปัญญาของแอปพลิเคชันอื่นๆ เพื่อล่วงรู้หรือให้ความสามารถในการนำไปใช้โดยไม่ได้รับอนุญาต.

การละเมิดความเป็นส่วนตัว: การนำข้อมูลส่วนตัวของผู้ใช้ไปใช้โดยไม่ได้รับอนุญาต, เช่นการเข้าถึงแกลเลอรี, กล้อง, หรือข้อมูลส่วนตัว

การโจมตีทางด้านความปลอดภัยของแอปพลิเคชัน: การหลอกลวงหรือการโจมตีแอปพลิเคชันโดยการประพฤติตนเป็นแอปพลิเคชันถูกต้องเพื่อหลอกผู้ใช้

กรณีศึกษา

คดีเหยื่อมิจฉาชีพถูกหลอกลวงให้ติดตั้งแอปพลิเคชันไม่พึงประสงค์ในอุปกรณ์สื่อสารเคลื่อนที่จนทำให้เสียทรัพย์

กรณีที่ 1:

ผู้เสียหายถูกหลอกให้ติดตั้งแอปพลิเคชันของหน่วยงานราชการ

อุปกรณ์: โทรศัพท์เคลื่อนที่ ระบบปฏิบัติการ Android

ช่องทางการติดต่อ: ผ่านการสนทนาในแอปพลิเคชัน “LINE”

เมื่อทำการตรวจสอบ พบว่าไฟล์ที่ส่งมาให้ทำการดาวน์โหลดและติดตั้งดังกล่าวไม่ปลอดภัย

15 / 66

Community Score

15 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

5ae4f9daeb31c691c03a781dceeb6d390b7280a66eadbca970cf1487536e0a46

29acb406066014539abcb9fa112fbce5.virus

android apk contains-elf

Size 18.73 MB

Last Analysis Date 5 hours ago

APK

DETECTION DETAILS RELATIONS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.fakeapp/flpv

Threat categories trojan banker

Family labels fakeapp flpv golddig

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Android.Banker.1208907	Avast-Mobile	Android:Evo-gen [Trj]
Avira (no cloud)	ANDROID/Golddig.FLPV.Gen	BitDefenderFalx	Android.Trojan.SpyAgent.HM
Cynet	Malicious (score: 99)	ESET-NOD32	A Variant Of Android/Packed.Jiagu.K Pot...
F-Secure	Malware.ANDROID/Golddig.FLPV.Gen	Fortinet	Riskware/Jiagu!Android
Google	Detected	Ikarus	Trojan-Spy.AndroidOS.Banker
K7GW	Trojan (005a905d1)	Kaspersky	HEUR:Trojan-Spy.AndroidOS.FakeApp.u
Symantec Mobile Insight	AdLibrary:Generisk	Trustlook	Android.Malware.General (score:7)
ZoneAlarm by Check Point	HEUR:Trojan-Spy.AndroidOS.FakeApp.u	Acronis (Static ML)	Undetected
Alibaba	Undetected	AI Yac	Undetected

Permissions

- ⚠ android.permission.CHANGE_NETWORK_STATE
- ⚠ android.permission.DISABLE_KEYGUARD
- ⚠ android.permission.INTERNET
- ⚠ android.permission.ACCESS_FINE_LOCATION
- ⚠ android.permission.SEND_SMS
- ⚠ android.permission.WAKE_LOCK
- ⚠ android.permission.WRITE_EXTERNAL_STORAGE
- ⚠ android.permission.RECORD_AUDIO
- ⚠ android.permission.WRITE_SETTINGS
- ⚠ android.permission.READ_PHONE_STATE

Activities

- com.xingchat.android.activity.SplashActivity
- cn.hx.plugin.ui.pwccma0.Kcyuha0Activity
- cn.hx.plugin.ui.pwccma0.Sbhsmb1Activity
- cn.hx.plugin.ui.pwccma0.Plrykc2Activity
- cn.hx.plugin.ui.kezaeb1.Xjhcha0Activity
- cn.hx.plugin.ui.kezaeb1.Oldkbb1Activity
- cn.hx.plugin.ui.kezaeb1.Yuzrhc2Activity
- cn.hx.plugin.ui.ftwmnc2.Cioopa0Activity
- cn.hx.plugin.ui.ftwmnc2.Molvxb1Activity
- cn.hx.plugin.ui.ftwmnc2.Zafflc2Activity

MITRE ATT&CK Tactics and Techniques

Defense Evasion TA0030

Obfuscated Files or Information T1406
Obfuscates method names

Discovery TA0032

Location Tracking T1430
Has permission to query the current location

Impact TA0034

Carrier Billing Fraud T1448
Has permission to send SMS in the background

Collection TA0035

Audio Capture T1429
Has permission to record audio in the background

Location Tracking T1430
Has permission to query the current location

Network Effects TA0038

Exploit SS7 to Redirect Phone Calls/SMS T1449
Has permission to send SMS in the background

กรณีศึกษา

กรณีที่ 2:

ผู้เสียหายได้รับ ข้อความ (SMS) “คืนเงินประกันการใช้ไฟฟ้าส่วนภูมิภาค PEA ยืนยัน การลงทะเบียน เงื่อนไขการขอคืนเงินประกันฯ สอบถามเพิ่มเติมที่ bit.ly/3MJYKjd”

เมื่อตรวจสอบเว็บไซต์ดังกล่าว ด้วยเว็บไซต์ Virustotal.com พบรายละเอียดแจ้งเตือนว่าเป็น “phishing”

ผู้เสียหายได้รับ ข้อความ (SMS) พร้อมแนบลิงก์ต้องสงสัยมาด้วย

เมื่อตรวจสอบเว็บไซต์ดังกล่าว ด้วยเว็บไซต์ Virustotal.com พบรายละเอียดแจ้งเตือนว่าเป็น “phishing”

VirusTotal - URL - a05659d10d68a

virustotal - Google Search

virustotal.com/gui/url/a05659d10d68a2a48f6f5f0faadcacc5e85e23ac2fe0e43b4afe286acfe354c5

Mon

All Bookmarks

http://pea.id-th.cc/

Sign in

Sign up

Did you intend to search across the file corpus instead? **Click here**

10 / 90

Community Score

10 security vendors flagged this URL as malicious

Reanalyze | Search | Graph | API

http://pea.id-th.cc/
pea.id-th.cc

text/html

Status
200

Last Analysis Date
2 months ago

DETECTION | DETAILS | LINKS | COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

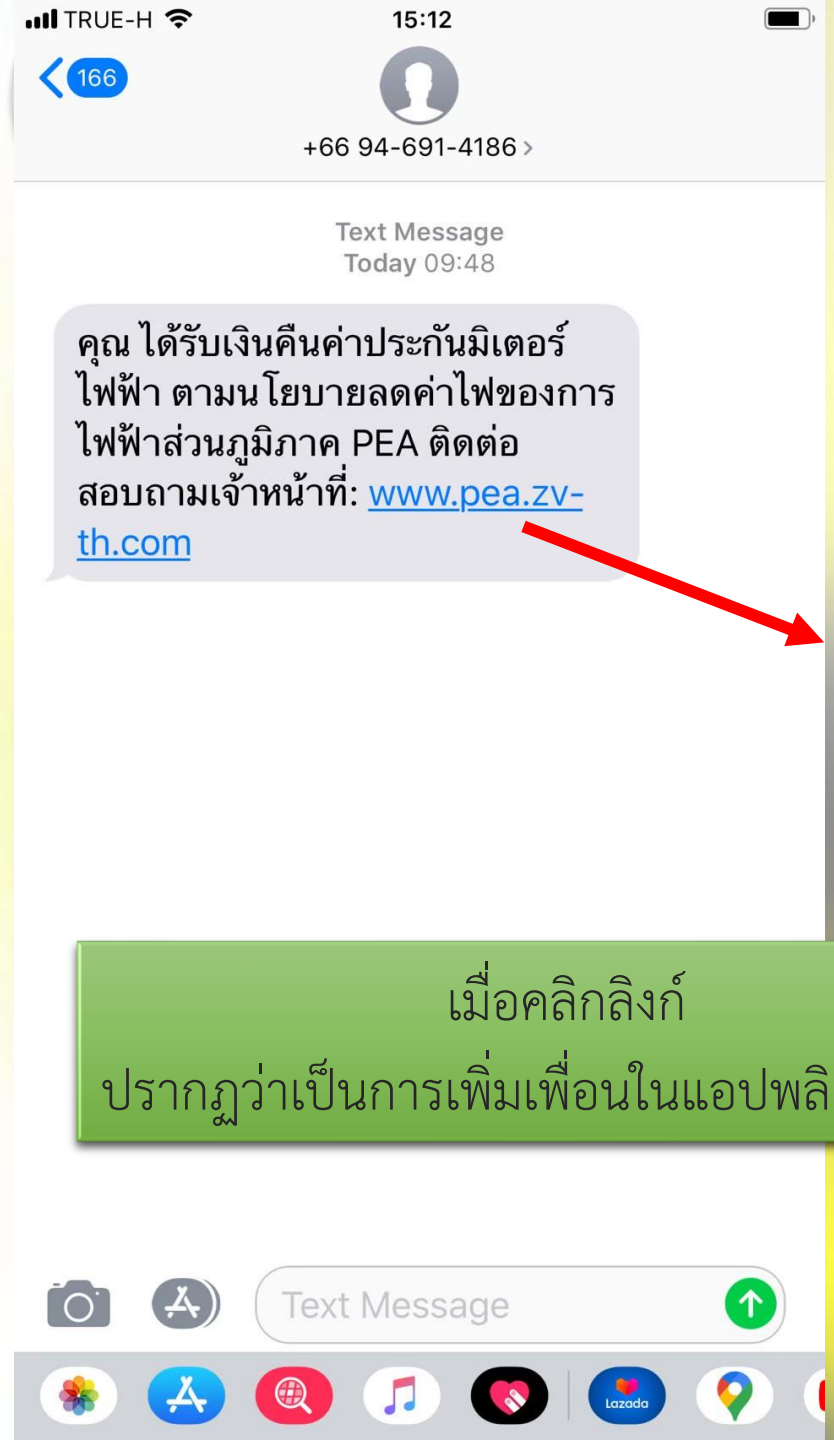
alphaMountain.ai	Phishing	Avira	Phishing
BitDefender	Malware	CyRadar	Malicious
Forcepoint ThreatSeeker	Phishing	Fortinet	Malware
G-Data	Malware	Lionic	Malware
SOCRadar	Phishing	Sophos	Malware
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean

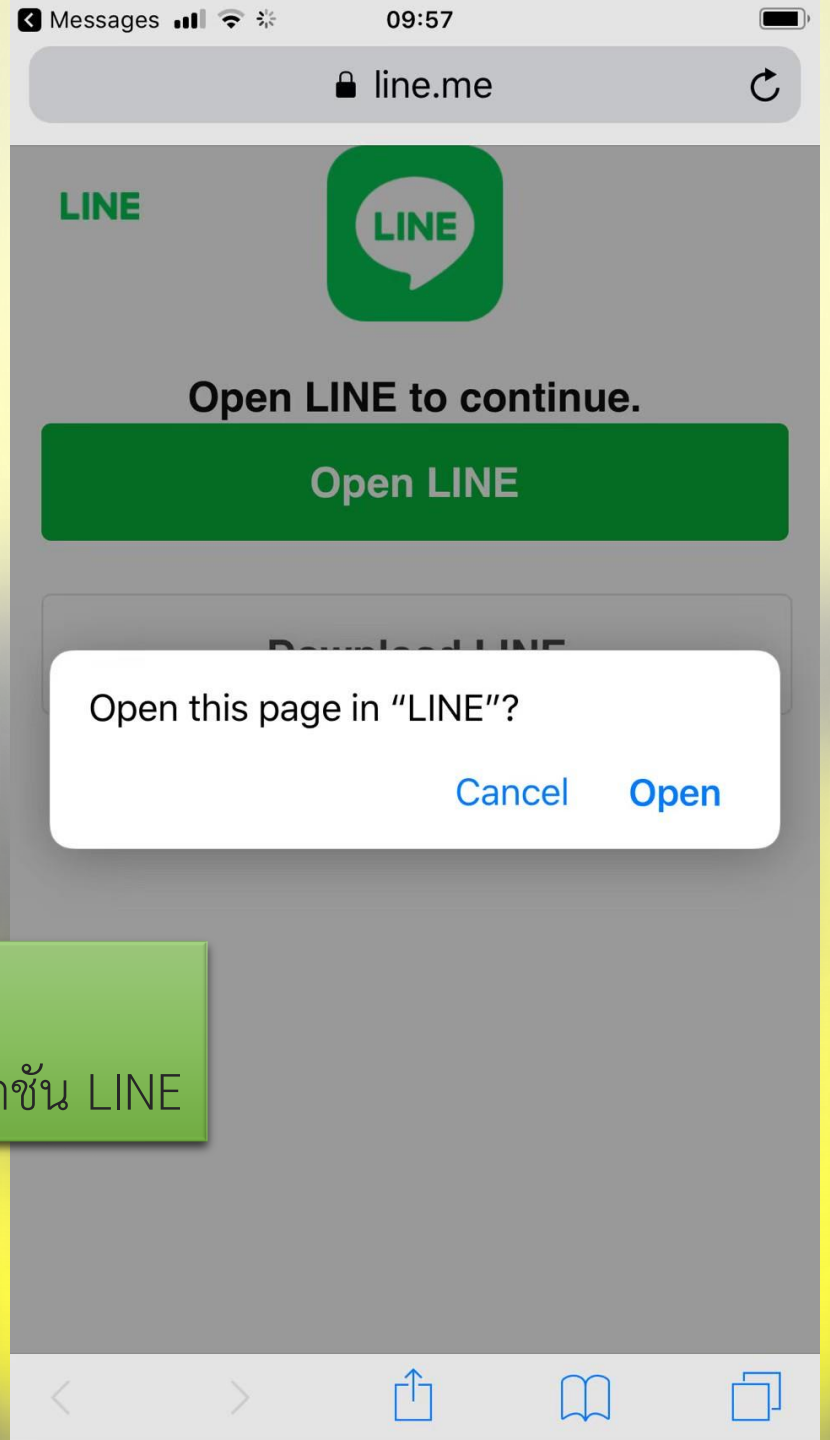
กรณีศึกษา

กรณีที่ 3:

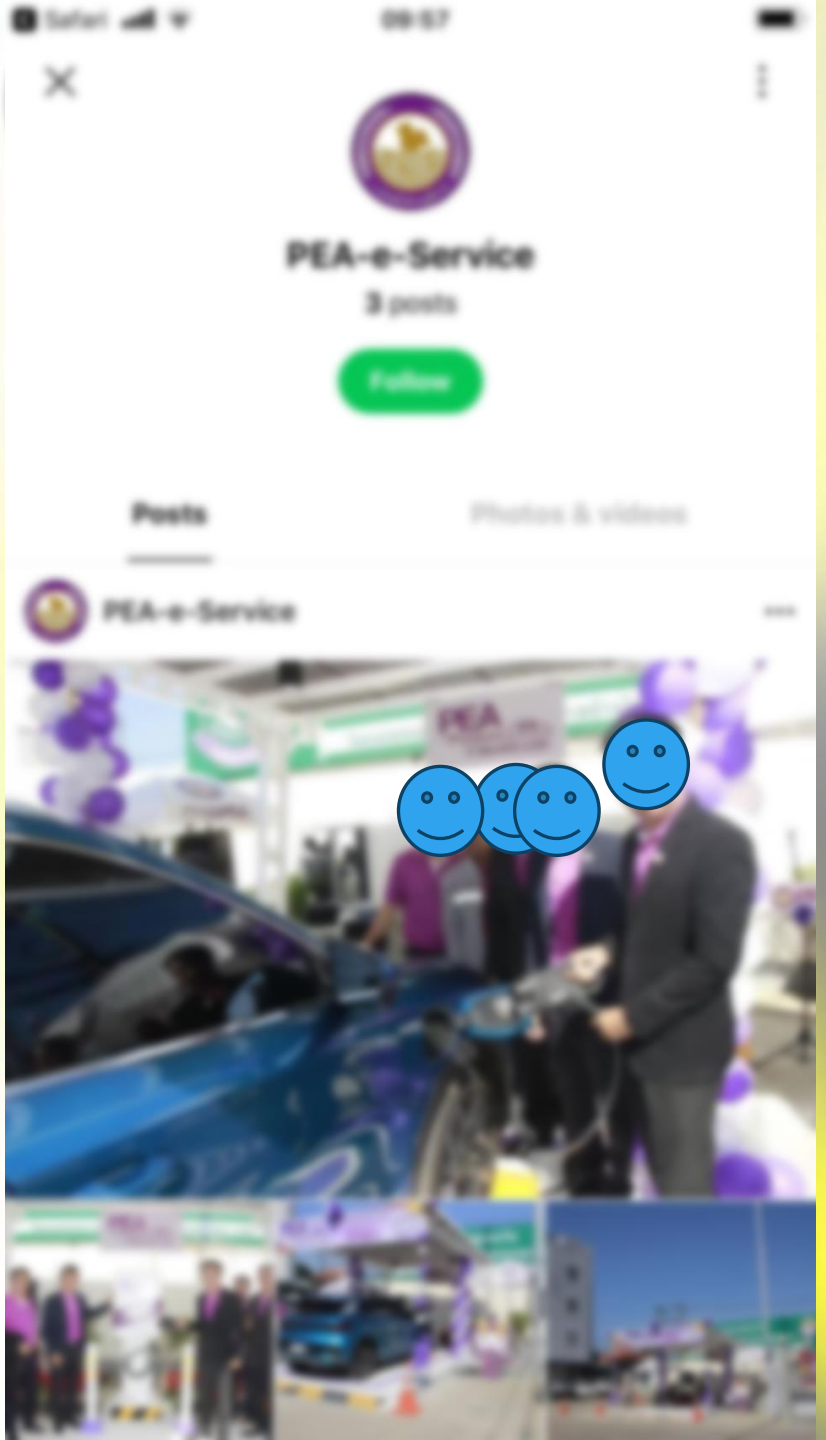
ผู้เสียหายได้รับการติดต่อจากกลุ่มบุคคลที่แอบอ้างว่า เป็นเจ้าหน้าที่ของรัฐหน่วยงานหนึ่ง โดยแจ้งข้อกล่าวหาว่ากำลังจะถูกดำเนินคดีฟอกเงิน พร้อมยื่นข้อเสนอเพื่อทำการช่วยเหลือให้พ้นคดี โดยต้องทำตามที่มิจฉาชีพแนะนำ เช่น การแจ้งข้อมูลทางการเงิน ข้อมูลส่วนบุคคล รวมถึงมีการโอนเงินไปรวบรวมไว้ยังบัญชีเดียว

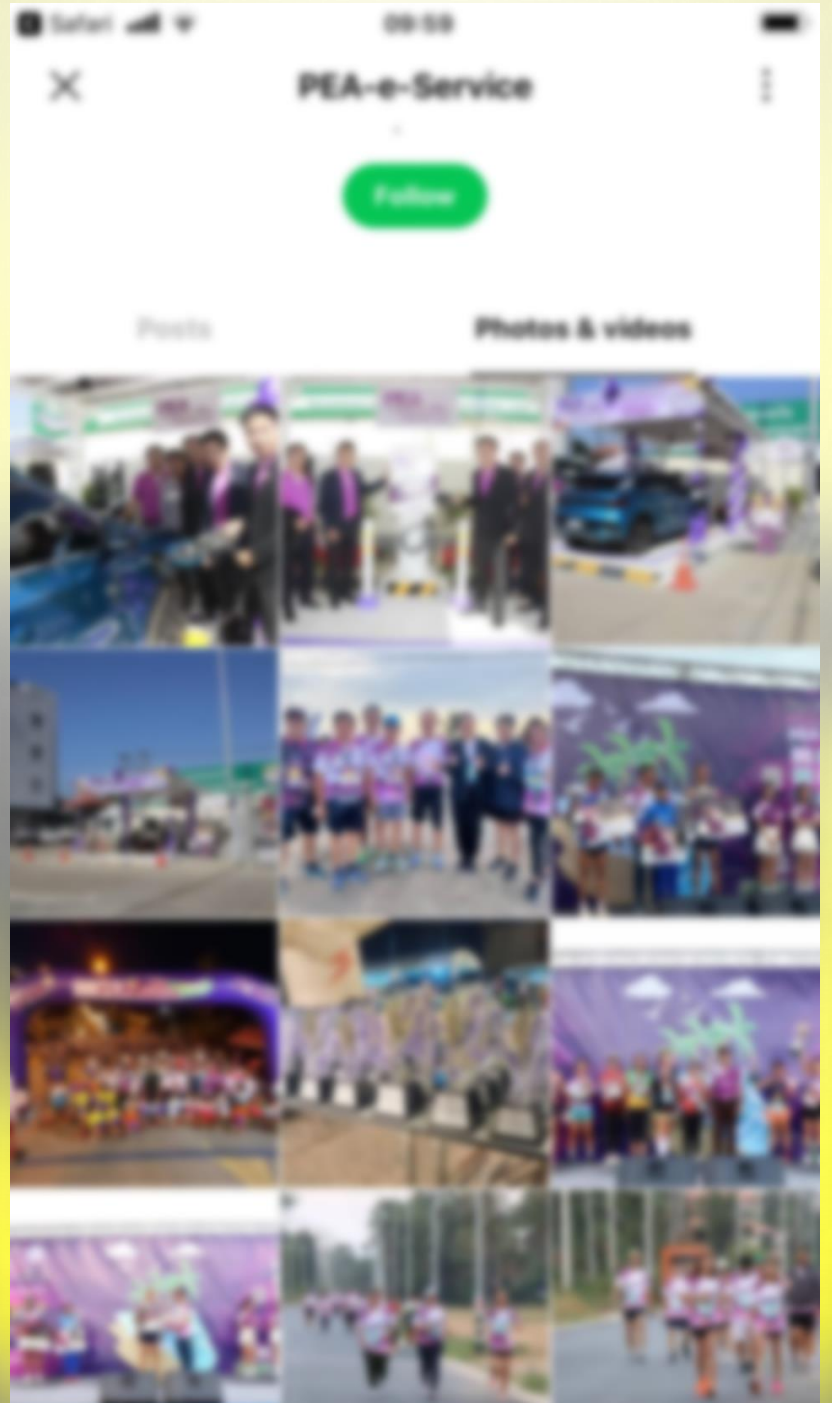
ตัวอย่างการส่งข้อมูลชักชวนผ่านทางสื่อทางโซเชียลต่างๆ





เมื่อคลิกลิงก์
ปรากฏว่าเป็นการเพิ่มเพื่อนในแอปพลิเคชัน LINE





Safari 09:57

PEA e-Service Follow

Posts Photos & videos

❗ PEA เตือนภัยมิจฉาชีพหลอกให้ลงทุนกองทุนรวมหุ้น ❗

ตามที่มีมิจฉาชีพเชิญชวนลงทุนในสื่อออนไลน์เรื่อง PEA เปิดโอกาสให้ลงทุนกองทุนรวมหุ้น ราคา เปิดพอร์ต 899 บาท ปันผล 250 บาทต่อวัน และ 3,099 บาท ปันผล 950 บาทต่อวัน

📣การไฟฟ้าส่วนภูมิภาค (PEA) ไม่มีนโยบายเชิญชวนให้ลงทุนรวมหุ้นใดๆ ในทุกช่องทาง

📌หากมีข้อสงสัย สามารถสอบถามข้อมูลเพิ่มเติมได้ที่สำนักงานการไฟฟ้าส่วนภูมิภาคในพื้นที่ หรือ 1129 PEA Contact Center ตลอด 24 ชั่วโมง

ข่าว / ภาพ : กองสื่อสารภาพลักษณ์องค์กร ดูน้อยลง

TRUE-H 14:54

99+ A-e-Service

คืนเงินประกัน

⚡ยินดีต้อนรับสู่ PEA Thailand⚡
เรายกการไฟฟ้ามาไว้ในมือคุณ ให้คุณได้ใกล้ชิดกับทุกบริการและเข้าถึงข่าวสารได้ไวกว่าที่เคย เพราะคุณจะได้พบกับสาระน่ารู้แบบจัดเต็ม รับรองว่าจะช่วยให้คุณใช้ไฟฟ้าได้อย่างปลอดภัยแถมประหยัดไฟอีกด้วย! 10:01

ขณะนี้เจ้าหน้าที่อยู่ระหว่างให้บริการท่านอื่นอยู่ เพื่อความรวดเร็วในการให้บริการ ท่านสามารถแจ้งประเด็นที่ต้องการติดต่อ รบกวนแจ้ง
-ชื่อ-นามสกุล
-เบอร์โทรศัพท์
-หมายเลขผู้ใช้ไฟฟ้า
-รหัสเครื่องวัดไฟ
เพื่อง่ายต่อการทำการตรวจสอบด้วยนะครับ 10:01

Unread messages below

ไม่ทราบว่าสะดวกให้ข้อมูลไหมครับ 10:31

Missed 14:07

Aa

TRUE-H 21:29

99+ A-e-Service

ไม่ทราบว่าสะดวกให้ข้อมูลไหมครับ 10:31

Missed 14:07

[redacted]

ไม่เป็นไรครับ 14:57

เดี๋ยวเจ้าหน้าที่ขอข้อมูลเบื้องต้นก่อนนะครับเพื่อทำการตรวจเช็คสิทธิ์ให้นะครับ 14:58

ข้อมูลเบื้องต้นนะครับ
-ชื่อ-นามสกุล
-เบอร์โทรศัพท์ 14:58

Unread messages below

ไม่ทราบว่าสะดวกไหมครับ 17:32

18:14

Aa

TRUE-H 19:18

99+

นะครับเพื่อทำการตรวจเช็คสิทธิ์ให้นะครับ 14:58

ข้อมูลเบื้องต้นนะครับ
-ชื่อ-นามสกุล
-เบอร์โทรศัพท์ 14:58

ไม่ทราบว่าสะดวกไหมครับ 17:32

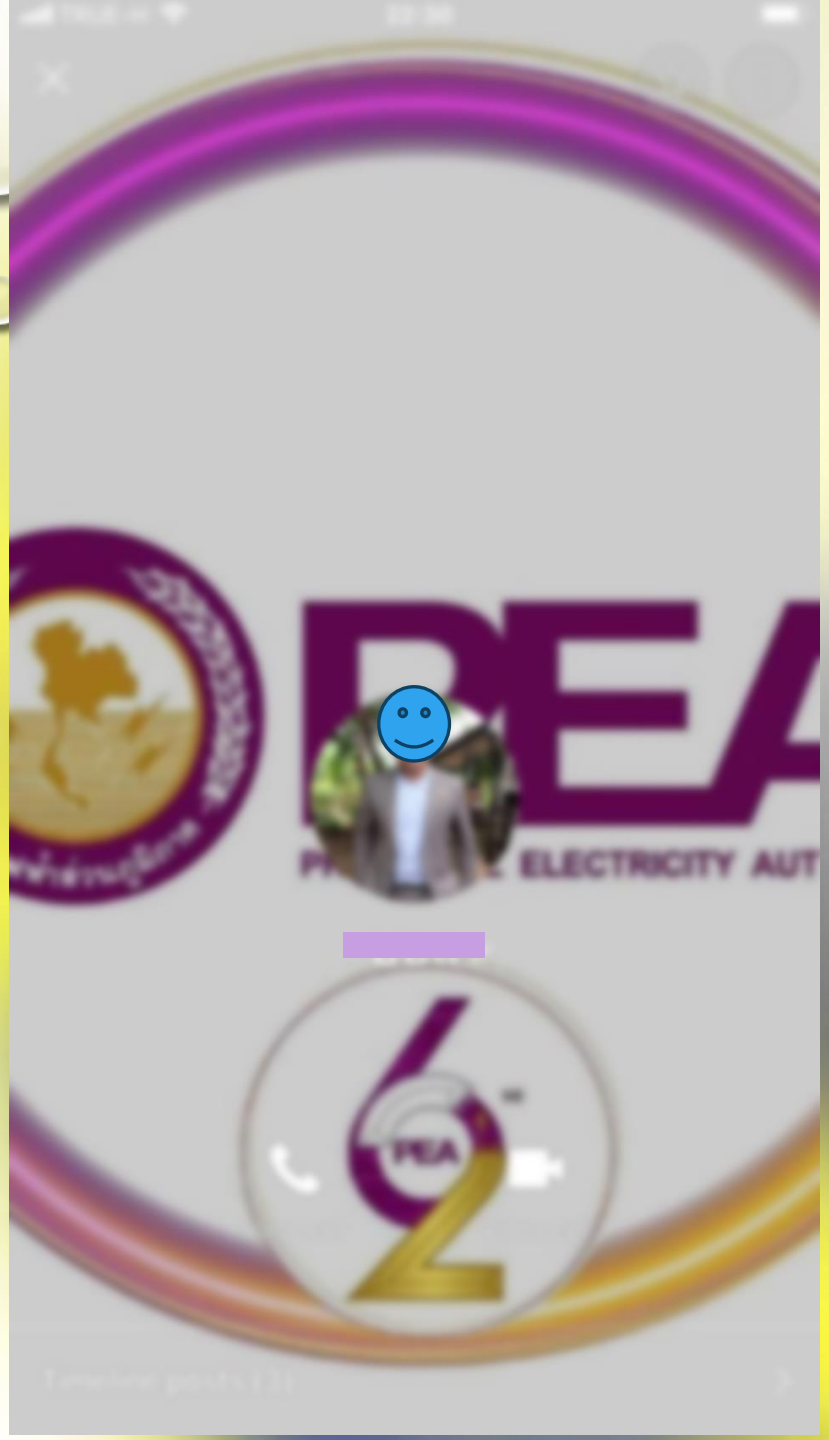
18:14

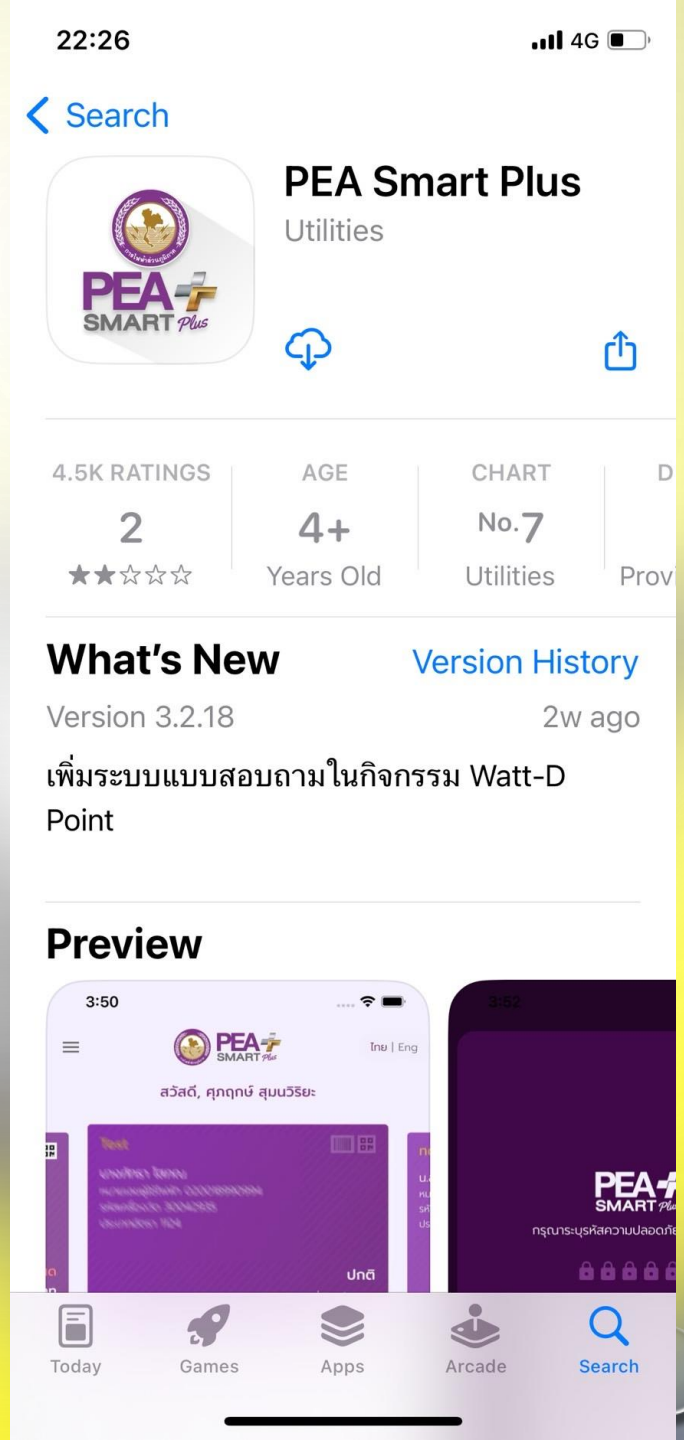
Fri, 05/01

Unread messages below

สวัสดีครับ 🙏 ไฟฟ้าส่วนภูมิภาค วันนี้คุณลูกค้าต้องการใช้บริการด้านไหนดีครับ พิมพ์หมายเลขแล้วแจ้งมาได้เลย ✨
✨ พิมพ์ "1"บิลค่าไฟหายเชคค่าไฟชำระค่าไฟ
✨ พิมพ์ "2" งานบริการขอใช้ไฟฟ้า
✨ พิมพ์ "3" งานบริการแอพพลิเคชั่น PEA SMART Plus 10:08

Aa





ดาวน์โหลดแอปพลิเคชัน
จากแหล่งที่น่าเชื่อถือเท่านั้น
App store
Play store

TRUE-H 13:52

150

02-182-0545 >

Fri, 17 Nov 14:37

เงินเข้า 500 บาท กดรับ *158# โทรออก สมัครลุ้นเลขเด่นดวงดี 3บ./ขค.

Sun, 26 Nov 09:28

ด่วน!ค่าโทรหมดกด*158# สมัครดวงดีลุ้นรับค่าโทรฟรี 500บาท3บ/ขค

Sat, 16 Dec 08:39

มีเงินเข้า 500 บาท กดรับ *158# โทรออก สมัครลุ้นเลขเด่นดวงดี 3บ./ขค.

Fri, 5 Jan 10:16

เงินเข้าโทรศัพท์ฟรี 500บาท กด*158# ลุ้นก่อนใคร สมัครดวงดีดวงเฮง 3บ/ขค

Text Message

TRUE-H 18:59

148

Text Message
20 Jan 2564 06:46

[redacted]vation Code (GAC). It expires in 2 minutes. Do not share it with anyone.

Tue, 7 Mar 16:20

ยินดีด้วย! คุณเป็นผู้โชคดีได้บัตรกำนัลเข้าพักโรงแรม 3 วัน 2 คืน ฟรี* ติดต่อรับได้ที่ grab-th-line.cc

Messages 18:59

goatbet-90.com

GOATBET90

แจกเครดิตฟรี 100

goat90 แจก โปรโมชั่นเด็ด ฝาก 19 รับ 100 ยังไม่พอ !! ฝาก 50 รับ 100 เลือกรับได้เลย

LINE ติดต่อแอดมิน คลิกที่นี่

สมัครสมาชิก รับเครดิตฟรี 100 คลิกเลย

พร้อมโปรโมชั่นอื่นๆ จาก goatbet มาให้เลือกอีกเพียบ !!!

ติดต่อแอดมิน คลิก !!

[redacted]

ฟรี 100

[redacted]

แชท

สมัครสมาชิก

Messages 07:25

vvip.pro-wow24hr.xyz

แชท

สมัครสมาชิก

TRUE-H 07:25

150

CUTESHOP >

Text Message
Fri, 2 Jun 07:17

WOW24HR. ต้อนรับต้นเดือน รับฟรี 100บ. เฉพาะวันนี้ bit.ly/hr24wk

TRUE-H 18:58

148

VMANA >

Text Message
Tue, 16 Jan 20:05

ฟรี 100
ไม่ต้องเติมก่อน ไม่แชร์
สมัครใหม่รับ 100%
bit.ly/90-goat

TRUE-H 07:25

151

+66 80-436-6937 >

Text Message
Sat, 10 Jun 12:55

แจก 100 ถอนได้ 1000 มีจำกัด
กดรับ https://bit.ly/40Lul7X

151

tgram >

Text Message
Sun, 25 Jun 18:04

คุณคือผู้โชคดีได้รับเตาอบไฟฟ้าฟรี ติดต่อรับรางวัลที่นี่คลิก
loan880.com

Text Message

ข้อแนะนำ การระวังตัว

https://www.virustotal.com/

Who’s call

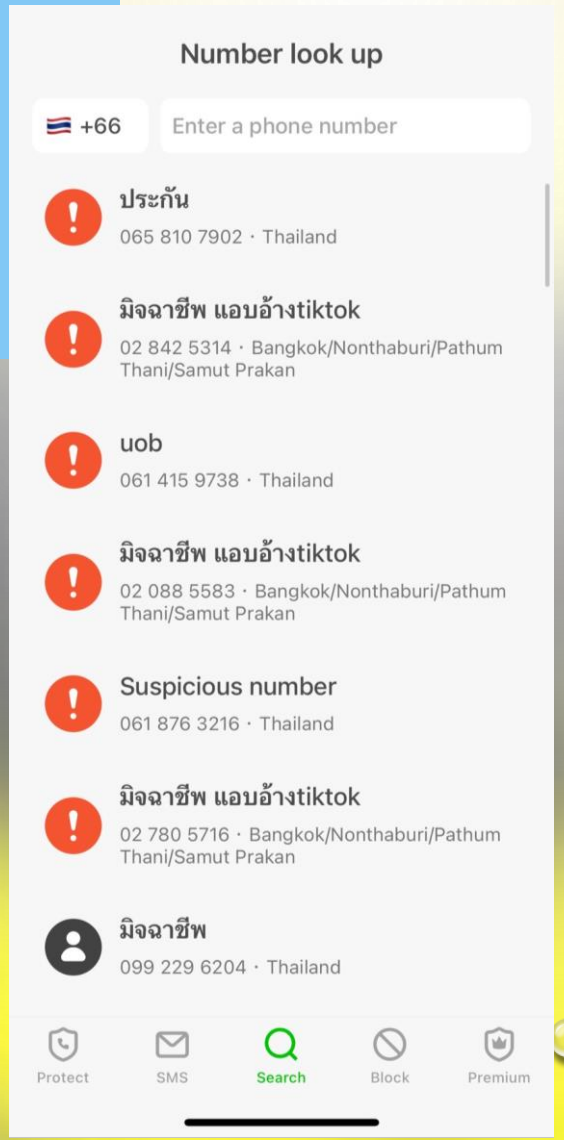
กรณี Facebook ให้ดูที่ bluetick

ใน LINE Open chat ให้ดูมงกุฎที่ admin

แต่ก็ปลอมได้แหละ

หมั่น Update ซอฟต์แวร์ให้ทันสมัย

AVG Mobile Security



กรณีโดนหลอก ต้องทำยังไง

https://thaipoliceonline.go.th

AOC 1441

วิธีป้องกันแอปดูดเงิน ดังนี้

1. ไม่ดาวน์โหลดโปรแกรมจากแหล่งอื่น นอกจากแหล่งที่ได้รับการควบคุมและรับรองความปลอดภัยจากผู้พัฒนาระบบปฏิบัติการที่เป็น Official Store อาทิ Play Store หรือ App Store เท่านั้น
2. ไม่ตั้ง password ซ้ำ หรือ ใช้ร่วมกับ Mobile Banking
3. ไม่ทำการสแกนใบหน้า หรือยืนยันตัวตนผ่านแอปพลิเคชันที่ไม่รู้จัก
4. ไม่กดลิงก์จาก SMS แปลกปลอม โดยธนาคารไม่มีนโยบายส่งข้อความ SMS แนบลิงก์ทุกชนิด หรือมีข้อความให้แอด Line ID หากได้รับ SMS ดังกล่าว อย่าหลงเชื่อเด็ดขาด
5. ควรสังเกตโล่ ที่อยู่ด้านหน้า Line account เสมอ ซึ่งควรมีโล่สีเขียว หรือน้ำเงินเข้ม เท่านั้น
6. หากต้องการทำธุรกรรมใด ๆ ควรโทรฯ กลับไปที่หน่วยงานที่ถูกแอบอ้างด้วยตนเอง
7. ไม่ควรให้ข้อมูลส่วนตัว เช่น หมายเลข 13 หลัก ผ่านทางโทรศัพท์
8. โทรแจ้ง 1441 สามารถโทร.แจ้งระงับอายัดบัญชีคนร้าย

ที่มา: https://www.tba.or.th/

Reference:

1. https://www.virustotal.com/
2. https://thaipoliceonline.go.th
3. https://www.tba.or.th/

สติ

สติ

สติ

สติดี ก็มีสตางค์ สติพัง สตางค์ก็หมด